Cybersecurity of quantum computers

Abstract: Quantum computing (QC) has the potential to transform numerous application domains by addressing classically intractable problems. However, its growing presence in cyberspace has introduced new security and privacy challenges. Similar to classical computing systems, the QC stack including software and hardware relies extensively on third parties, many of which are emerging and trust-seeking or less-trusted. This stack often contains sensitive intellectual property (IP) that demands protection. Given the high cost and limited availability of likely trustworthy quantum hardware, users may be enticed to explore emerging and trust-seeking but cheaper and readily available quantum hardware, which can enable the stealth of IP and tampering of quantum programs and/or computation outcomes. Similarly, emerging compilation services may compromise circuit confidentiality. Despite the strategic significance of QC and its potential to process sensitive information, its security and privacy concerns remain underexplored. This talk, which requires no technical background on quantum computing, will provide a comprehensive overview of QC fundamentals, key vulnerabilities, recent attack vectors, and corresponding defenses. It will also illustrate open problems to build and strengthen the quantum security community.

Biography: Dr. Swaroop Ghosh holds a Ph.D. from Purdue University. Before joining academia, he worked as a Senior Research and Development Engineer at Intel Corp. He has published 10 book/book chapters and 230+ peer-reviewed papers and holds 15 US patents. Dr. Ghosh has received numerous awards for excellence in research, advising and teaching most notably DARPA Young Faculty Award and Director's Fellowship, ACM SIGDA Outstanding New Faculty Award, IEEE Computer Society's TCVLSI Mid-Career Award and NAGS Geoffrey Marshall Mentoring Award. He has also received 7 Best Paper Awards. Dr. Ghosh is a Fellow of IEEE, US National Academy of Inventors and International Academy of Artificial Intelligence Sciences (AAIS), elected member of National Academy of AI and a Distinguished Speaker of ACM. His current research interests include circuit design, hardware security and quantum computing.